UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,165	10/31/2003	Jonathan D. Herbach	07844-623001	1607

21876 7590 11/17/2008

FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DUNN, DARRIN D	

ART UNIT	PAPER NUMBER
2121	

NOTIFICATION DATE	DELIVERY MODE
11/17/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/699,165	HERBACH ET AL.	
	Examiner	Art Unit	
	DARRIN DUNN	2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) *9-22 and 30-34* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 23-29, 35-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/28/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the communication filed 07/28/2008.

2. Claims 1-42 are pending. Claims 9-22 and 30-34 have been cancelled.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 07/28/2008 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 1 recites the limitation " the authentication program" in line 14, but previously recites "a software program." There is insufficient antecedent basis for this limitation in the claim.

6. Claim 1 recites "response to the request" in line 11. Line 2 recites "a request." Line 9 recites "update request." There is insufficient antecedent basis for this limitation in the claim.

7. Claim 23 recites "the authentication program" but previously recites a software program. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 1,3-4, 23,25,28, 36-37, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kobata et al. (USPN 2002/0077986).

11. As per claim 1, Kobata et al. teaches a method comprising:

receiving, at a server, a request from a client to take an action with respect to an electronic document ([0236] e.g., receiving system makes a request to obtain a digital asset);

retrieving a document identifier from the request ([Figure 2 0 elements 105, 115, 220], [0131] e.g., content ID associated with individual copies of the digital content would also be illustrative that certain rights are associated with particular digital content);

determining whether user authentication is needed based on the document identifier and the action ([0013-16], [0027], [0236] e.g. the rights sections includes a description of who is authorized to change the rights…User authentication is interpreted as including the right of a

user to manipulate digital content, and as best understood, user authorization is required to assure that digital content rights are correctly associated with users authorized receive the digital content) ;

subsequent to retrieving the document identifier, sending information specifying an acceptable authentication procedure ([0027-29], [0252] e.g., An authentication procedure is interpreted as any step used in enabling a user to access and/or manipulate a digital asset. As part of the procedure, rules are defined, further including the step of providing a viewer, to control access to a digital asset rights defining how the digital asset may be manipulated are also transmitted to the receiving computer, and the digital asset is stored at the receiving computer. The viewer further can perform the authorization, identification, and password authentication, as in the case of an upgrade procedure;)

receiving an authentication procedure update request from the client, the authentication procedure update request associated with the electronic document ([0031], [Fig 7] e.g., end user requests modification of digital rights. In response, digital rights may be updated upon granting the request);

obtaining, at the server and in response to the request, a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the authentication procedure ([0236], [0121] , [0252] e.g., upon verifying the request, the gatekeeper, i.e., server, determines the appropriate viewer, i.e., obtaining a software program. The viewer is operable to "effect the authentication procedure" via interacting with the rules and enabling access to a digital asset – the viewer module is "operable" to invoke a procedure to provide authentication information -0252 lines 12-15. Note: the authentication program is silent

as to what it is identifying. Here, the module controls what a user is able to present and in addition authenticates any potential upgrades); and

However, Kobata et al. does not expressly teach that in response to the request (note: is the request responsive to the updated request or request with respect to the electronic document?) for digital content, the authentication program is sent to the client for use in identifying a current user and controlling the action. Kobata et al. does teach the ability to a) upgrade the viewer via a user ([0252]), b) require the user to upgrade the viewer ([0113).

Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to provide the ability to upgrade the viewer module. The viewer modules provides for "a use" in identifying a user (e.g., password required during an upgrade request) and controlling the action with respect to the electronic document and document permissions (e.g., view settings). However, the main issue us whether it would have been obvious to send the authentication program, i.e., updated viewer, responsive to the request with respect to the electronic document. Since a request for an electronic document entails checking for potential updates to the viewer module, it would have been obvious to one of ordinary skill in the art to check for updates subsequent to the request with respect to the electronic document to ensure data consistency. (Original) The method of claim 1, wherein obtaining the software program comprises requesting and receiving the software program from a second server.

12. As per claim 3, Kobata et al., as modified, teaches a method comprising:

receiving, at a server, a request from a client to take an action with respect to an electronic document [0236] e.g., receiving system makes a request to obtain a digital asset);

obtaining, at the server and in response to the request, a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure (procedure ([0236], [0121] , [0252] e.g., upon verifying the request, the gatekeeper, i.e., server, determines the appropriate viewer, i.e., obtaining a software program. The viewer is operable to "effect the authentication procedure" via interacting with the rules and enabling access to a digital asset – the viewer module is "operable" to invoke a procedure to provide authentication information -0252 lines 12-15. Note: the authentication program is silent as to what it is identifying. Here, the module controls what a user is able to present and in addition authenticates any potential upgrades);

sending the authentication program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document ([0252] e.g., upgraded viewer is interpreted as requiring a newer version of a viewer module be installed on the end-user device);

receiving an updated authentication procedure, the updated authentication procedure associated with the electronic document ([0031], [Fig 7] e.g., end user requests modification of digital rights. In response, digital rights may be updated upon granting the request);

However, Kobata et al. does not teach receiving a subsequent request from the client to take the action with respect to the electronic document. Kobata et al. does teach a system where users may make requests for digital assets and further receive updates ([0252]).

Therefore, at the time the invention was made, one of ordinary skill in the could foresee that users would request new digital assets, and in effect, would repeat the aforementioned

limitations.

obtaining, in response to the subsequent request, a new software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the updated authentication procedure ([0252] e.g., based on the potential, repeated requests in view of a user receiving a either an upgraded viewer module and/or being forced to upgrade, it would have been obvious to enable the system to a) receive a request for digital content b) check for updates for a viewer during the request and c) repeat this process for subsequent requests) ; and

sending the new software program to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document ([0113], [0252] e.g., as modified, it is interpreted that in response to a request for digital content, i.e., association, a new version would be checked. In effect, it would have been obvious to check to for updates to a viewer during a request for digital content, especially given the need for consistency, see above. The new viewer module would be sent to the end-user)

13. As per claim 4, Kobata et al. teaches the method of claim 1, wherein the software program uses an existing interface provided by the client to communicate authentication information to the server ([0252] e.g., providing password authentication)

14. As per claim 23, Kobata et al., as modified, teaches a

a client that sends a request to a server when an action is to be taken with respect to an electronic document local to the client ([0236] e.g., receiving system makes a request to obtain a digital asset);

the server that receives the request, and in response to the client, the server obtains and sends a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure ([0252] e.g., as modified, in response to the request, it would have been obvious to check for an update as to ensure all modules are properly updated); and

wherein the client uses the authentication program to identify a current user and control the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document ([0252] e.g., password authentication involves user identification and in addition, the viewer controls whether content may be presented as a function of whether a user is permitted to access the module), and wherein the action comprises an action taken with respect to the electronic document subsequent to opening the electronic document at the client ([0253] e.g., the number of times content may be heard is a function of the number of times its has been opened)

15. As per claim 25, Kobata et al. teaches the system of claim 23, wherein the client includes a security handler that provides a server-communication interface to the software program ([0252] e.g., password authentication)

16. As per claim 28, Kobata et al. teaches the system of claim 23, wherein the server comprises:

a server core with configuration and logging components ([Figure 2 – element 115]);

an internal services component that provides functionality across dynamically loaded methods ([Figure 2- element 230); and

dynamically loaded external service providers, including an authentication service provider ([Figure 15 – elements 1402, 1406, 1410])

17. As per claim 36, Kobata et al. teaches the system of claim 23, wherein the server receives a subsequent request from the client to take the action with respect to the electronic document, obtains, in response to the subsequent request, a new authentication process, and sends the new authentication process to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document (supra claim 23 discussion pertaining to obvious modification of providing multiple requests, checking for an updated viewer module, and providing the updated viewer module. The viewer module operable to verify a user and control content presentation as a function of user rights associated with a digital asset)

18. As per claim 37, Kobata et al. teaches the method of claim 23, wherein the software program uses an existing interface provided by the client to communicate authentication information to the server ([0252] e.g., providing password authentication)

19. As per claim 42, Kobata et al. teaches the system of claim 23, wherein the server retrieves a document identifier from the request (([Figure 2 0 elements 105, 115, 220], [0131] e.g., content ID associated with individual copies of the digital content would also be illustrative that certain rights are associated with particular digital content), determines whether user authentication is needed based on the document identifier and the action ([figure 10 – element 1015), sends information specifying an acceptable authentication procedure ([0027] e.g. transmitting rights to end-user), and retrieves an authentication procedure update request from

the client (figure 7 -element 705])

19. Claims 5-6, 8, 26-27, 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kobata et al. (USPN 2002/0077986) in view over view of Hu (USPN 5586260), and in further view over Raciborski et al. (USPN 20050132083)

20. As per claims 5, 26-27, and 38, Kobata et al. teaches receiving credentials information from the client derived at least in part based on the input obtained by the client using the software program ([0252], [0075], [0016] e.g., password authentication associates a user and the user is associated with a description, i.e., credential - vice president)

However, Kobata et al. does not teach communicating with a third party authentication server to authenticate the current user based on the credentials information. Hu teaches a third party authentication server ([ABSTRACT])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to implement a third party authentication server as taught by Hu et al. Hu teaches a method for authenticating a client for a server. Since a third party authentication server provides a well known means in which to maintain, store, and retrieve credentials, it would have been advantageous to provide this server as an additional means, in effect providing both redundancy in addition to reducing load on the primary server.

21. As per claim 39, Kobata et al. teaches wherein the input obtained by the client comprises text input ([0252] e.g., password)

22. As per claim 40, Kobata et al. teaches a password authentication means but does not teach wherein the input comprises biometric data. Raciborski et al. teaches biometric data ([0043])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Kobata et al. to include biometric input in addition to password authentication. Biometric inputs are well known to authenticate a user, and therefore would have been a more accurate means of ensuring a user is properly authenticated before approving an upgrade to a viewer module, as taught by Kobata et al.

23. As per claim 6, Kobata et al. teaches the method of claim 5, wherein the input obtained by the client comprises text input ([0252] e.g., password)

24. As per claims 8 and 41, Hu teaches returning an access key from an authentication gateway acting as a proxy server to the client, i.e., receipt, based on credentials ([ABSTRACT], [COL 1 lines 58-63] e.g., receiving an authentication receipt from a third party authentication server)

25. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable under Kobata et al. (USPN 2002/0077986) in view over view of Hu (USPN 5586260), and in further view of over Raciborski et al. (USPN 20050132083).

26. As per claim 7, Kobata et al., as modified, teaches a password authentication means but does not teach where the input is obtained by the client comprising biometric data. Raciborski et al. teaches biometric data ([0043])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Kobata et al. to include biometric input in addition to password

authentication. Biometric inputs are well known to authenticate a user, and therefore would have been a more accurate means of ensuring a user is properly authenticated before approving an upgrade to a viewer module, as taught by Kobata et al.

27. Claims 2, 24, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kobata et al. (USPN 2002/0077986) in view over Kano et al. (USPN 20030135650)

28. As per claims 2 ,24, and 35, Kobata et al. does not teach a second server providing the software program. . Kano et al. teaches a backup server ([ABSTRACT])

Therefore, at the time the invention was made, it would have been obvious to have provided a backup server as taught by Kano et al. to provide fault tolerant system. In the event of a primary server failure, it would be advantageous to enable the software to be downloaded from a backup server as to enable continuous access to content.

29. Claim 29 is rejected under 35 U.S.C 103(a) as being unpatentable over Kobata et al. USPN 2002/0077986) in view over Raciborski et al. (USPN 20050132083), and in further view of Tenerelllo (USPN 7233981)

30. As per claim 29, Raciborski et al. teaches a business logic tier comprising a cluster of document control servers ([0029] e.g. content delivery networks); an application tier including the client comprising a viewer client, a securing client, and an administration client ([FIG 1-FIG 2A – client computer functions via providing a view – browser, securing – downloading the manager (securing a program), and administration (storage media)). However, Racoborski et l does not teach a load balancer that routes client requests to the document control server. Tenerello teaches a system and method for load balancing ([COL 1 lines 14-20], [COL 2 lines 63-67])

Therefore, at the time the invention was made, one of ordinary skill would have motivation to load balance a system. Raciborski et al. teaches that various user computers may access content objects ([0029]) Tenerello teaches a load balancing means in which multiple requests may be efficiently processed. Since load balancing increases performance of a system, it would have been obvious to have enabled a system employing multiple user computers, each requesting access to a resource, a means to load balance the requests as to optimize the system.

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure..

6487301

6751336

6615350

20020082997

20020077986

20020019943

20040177276

20060036548

Response to Amendment

32. The amendment, submitted, 07/28/08, has been entered and made of record.

Response to Arguments

33. Applicant's arguments with respect to claims 1-8, 23-29, and 35-42 have been considered but are moot in view of the new ground(s) of rejection.

A] Figure 7 depicts end-user requests modification of digital rights, i.e., updated authentication procedure. A need to modify a digital right may occur subsequent to a request for a digital asset. The Examiner reasons that a user, upon receiving digital content, may desire additional rights. In effect, modifying a digital right, subsequent to receiving digital content, would enable a user to ascertain a current level, whether or not the level is suitable, and subsequently request a modified digital right. Such rights granted may include manipulating a digital asset by a particular viewer, the viewer interacting with a database to control access to the digital asset. The motivation is supported via [0166-0167]

B] A gateway server, responsive to a request for content, obtains the appropriate viewer for outputting digital content. A typical viewer function includes modifying the displayed digital asset ([0241]). The viewer is understood as being operable to identify a user ([0252 e.g., passwords) and in effect "effects" an authentication procedure because the viewer enforces the rules associated with what and how a user may access digital assets (e.g., manipulation of a digital asset in view of a request to modify a digital right. It is understood that manipulation of a right will carry forward to the viewer, i.e., the viewer allows modification of a digital asset)

C] The viewer module may be updated in response to an upgrade request and/or the availability of an improved viewer application. The motivation to support downloading a new viewer application subsequent to a request for content is based on the need to check for updates. A

request for content is made, a newer version would be checked for, and subsequently installing an updated viewer. In the alternative, an upgrade request via the viewer module GUI provides an upgrade procedure, i.e., authentication program. The former view supports "sending the software program." The latter is understood as sending the "authentication program" because "sending", in this case, does not specify the source in contrast to the former.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DD
11/08/08

/Albert DeCady/
Supervisory Patent Examiner, Art Unit 2121